Nástroje a možnosti internetu

Internet jako nástroj sledování II.

1. 11. 2024

Minule:

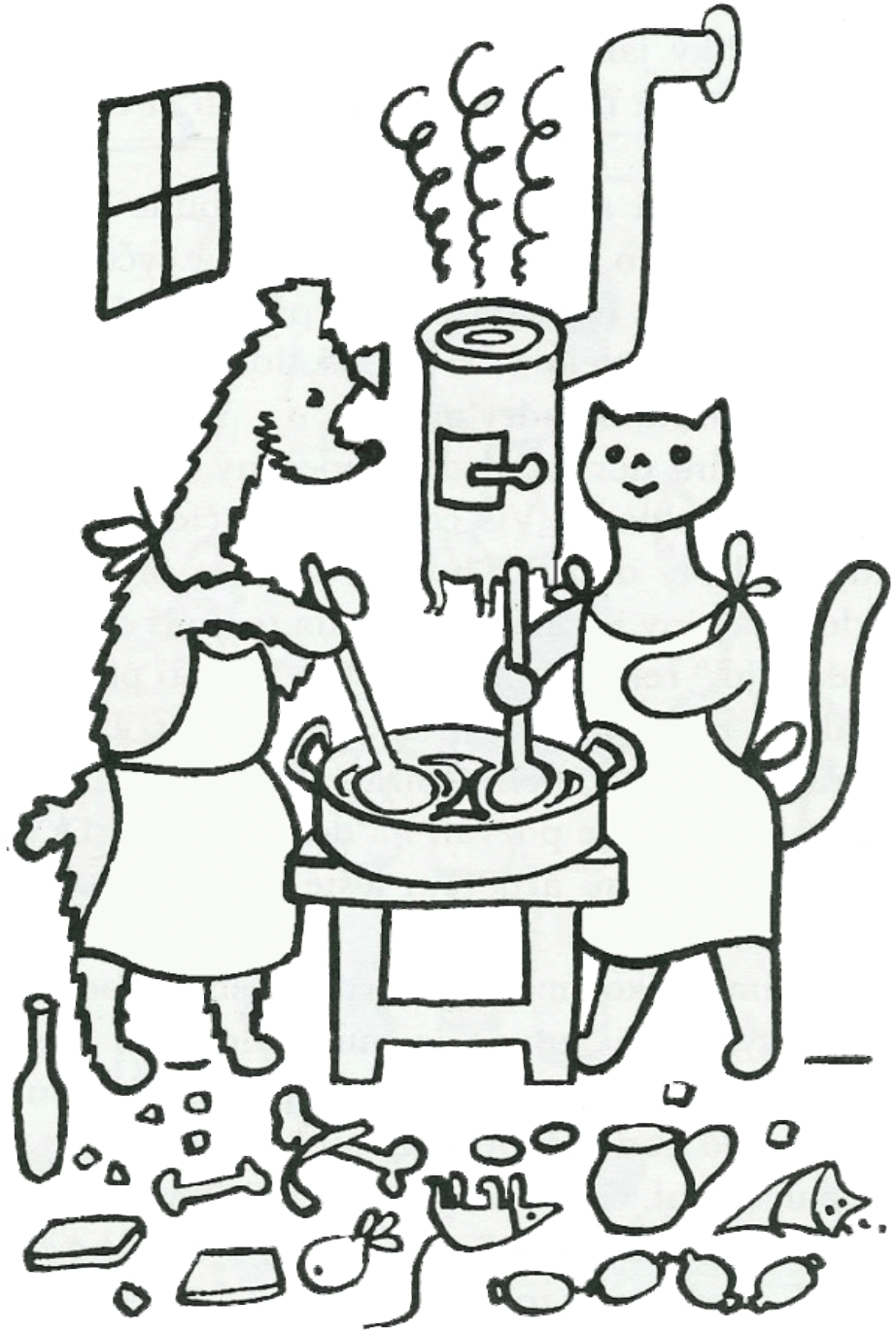
sledovací skripty

cookies třetích stran

browser fingerprinting

nové standardy typu *Topics API*

Vyzkoušeli jste
některé z testů
zmíněných minule?



paradox: *fingerprinting*

„Anonymní“ prohlížeče

- prohlížeče se striktním přístupem ke sledování
- většina blokací přímo zabudována
- otázkou je vždy model monetizace

Brave

Vivaldi

Epic

Mullvad

„Anonymní“ vyhledávače

- vyhledávače s odlišným modelem monetizace
- nesbírají data o uživatelích
- (ne)prodávají reklamní prostor

DuckDuckGo

MetaGer (a jeho konec)

Searx a SearXNG

Mojeek

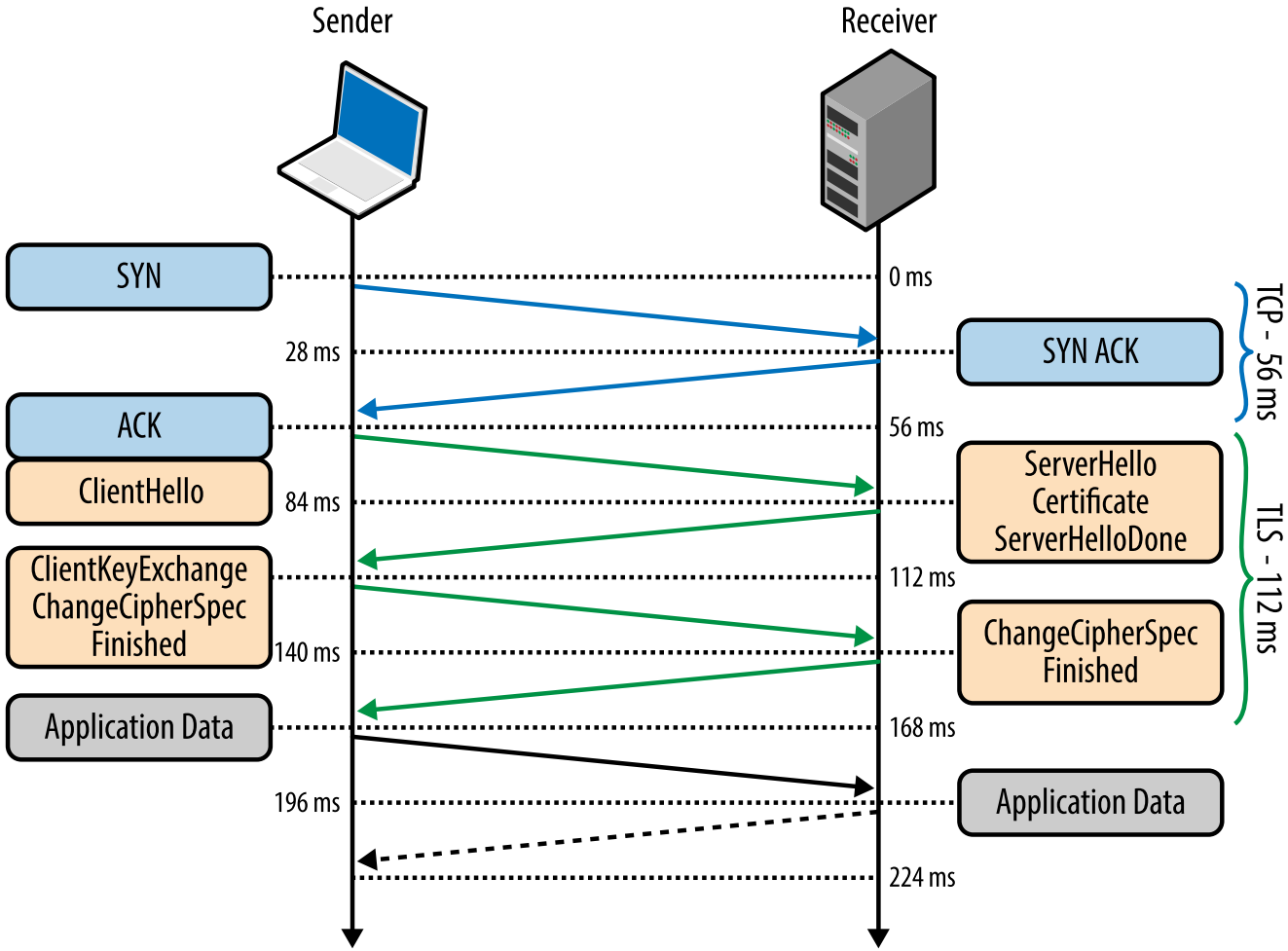
DuckDuckGo

HTTPS

HTTPS

- co je za potíže s HTTP?
- SSL/TLS a certifikace
- šifrované propojení
- HTTPS Everywhere *(už spíše nerelevantní)*

Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů



Zdroj: https://hpbn.co/

```
[2022/10/19 16:26] [...]
[2022/10/19 16:30] novinky.cz
[2022/10/19 16:35] idnes.cz
[2022/10/19 16:42] seznam.cz
[2022/10/19 16:43] google.cz
[2022/10/19 17:01] kocarky.cz
[2022/10/19 17:08] mimibazar.cz
[2022/10/19 17:30] google.cz
[2022/10/19 17:33] hnutiprozivot.cz
[2022/10/19 17:37] interupce.info
[2022/10/19 17:39] napocatku.cz
[2022/10/19 17:44] fnbrno.cz
[2022/10/19 18:01] mapy.cz
[2022/10/19 18:07] [...]
```

HTTPS

- nejde jen o obsah komunikace
- metadata jsou často mnohem cennější vhled

```
[2020/11/19 17:30] google.cz
[2020/11/19 17:33] hnutiprozivot.cz
[2020/11/19 17:37] interupce.info
[2020/11/19 17:39] napocatku.cz
[2020/11/19 17:44] fnbrno.cz
[2020/11/19 18:01] mapy.cz
```

HTTPS

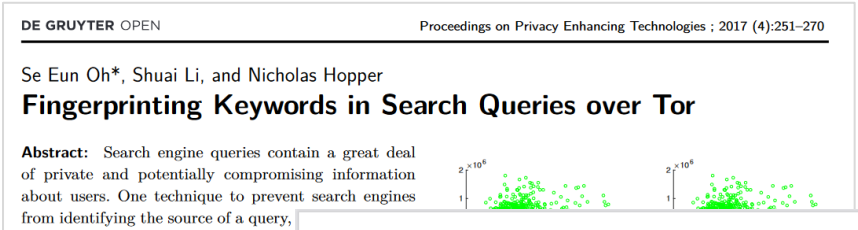
MITM a SSL hijacking

homograph attack

website fingerprinting

- *dá se to obejít?*
- *website fingerprinting*

  identifikace jednotlivých stránek
- odhadování *query* podle množství přenášených dat a rychlosti



DE GRUYTER OPEN Proceedings on Privacy Enhancing Technologies ; 2017 (4):251–270

Se Eun Oh*, Shuai Li, and Nicholas Hopper

Fingerprinting Keywords in Search Queries over Tor

Abstract: Search engine queries contain a great deal of private and potentially compromising information about users. One technique to prevent search engines from identifying the source of a query, vice providers (ISPs) from identifying queries is to query the search engine mous network such as Tor.

In this paper, we study the extent t Fingerprinting can be extended to finge queries or keywords to web applicatio Keyword Fingerprinting (KF). We sh menting traffic analysis using a two-sta new task-specific feature sets, a passiv sary can in many cases defeat the use search engine queries.

RESEARCH-ARTICLE

Touching from a distance: website fingerprinting attacks and defenses

Authors: Xiang Cai, Xin Cheng Zhang, Brijesh Joshi, Rob Johnson Authors Info & Affiliations

Publication: CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security • October 2012 • Pages 605–616 • https://doi.org/10.1145/2382196.2382260

112 1,216 Get Access

ABSTRACT

We present a novel web page fingerprinting attack that is able to defeat several recently proposed defenses against traffic analysis attacks, including the application-level defenses HTTPOS and randomized pipelining over Tor. Regardless of the defense scheme, our attack was able to guess which of 100 web pages a victim was visiting at least 50% of the time and, with some defenses, over 90% of the time. Our attack is based on a simple model of network behavior and out-performs previously proposed ad hoc attacks. We then build a web site fingerprinting attack that is able to identify whether a victim is visiting a particular web site with over 90% accuracy in our experiments.

2012 IEEE Symposium on Security and Privacy

Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail

Kevin P. Dyer*, Scott E. Coull†, Thomas Ristenpart‡, and Thomas Shrimpton*

*Department of Computer Science, Portland State University, Portland, USA. Email: {kdyer, teshrim}@cs.pdx.edu

† RedJack, LLC., Silver Spring, MD, USA Email: scott.coull@redjack.com

‡Department of Computer Sciences, University of Wisconsin-Madison, USA. Email: rist@cs.wisc.edu

ract—
consider the setting of HTTP traffic over encrypted , as used to conceal the identity of websites visited ser. It is well known that traffic analysis (TA) attacks curately identify the website a user visits despite the encryption, and previous work has looked at specific countermeasure pairings. We provide the first com- sive analysis of general-purpose TA countermeasures. w that nine known countermeasures are vulnerable to attacks that exploit coarse features of traffic (e.g., to- e and bandwidth). The considered countermeasures ones like those standardized by TLS, SSH, and and even more complex ones like the traffic morphing of Wright et al. As just one of our results, we show spite the use of traffic morphing, one can use only pstream and downstream bandwidth to identify — % accuracy— which of two websites was visited. One tion of what we find is that, in the context of website cation, it is unlikely that bandwidth-efficient, general- e TA countermeasures can ever provide the type of y targeted in prior work.

words-traffic analysis countermeasures; privacy; ma- earning; padding; encrypted traffic

I. Introduction

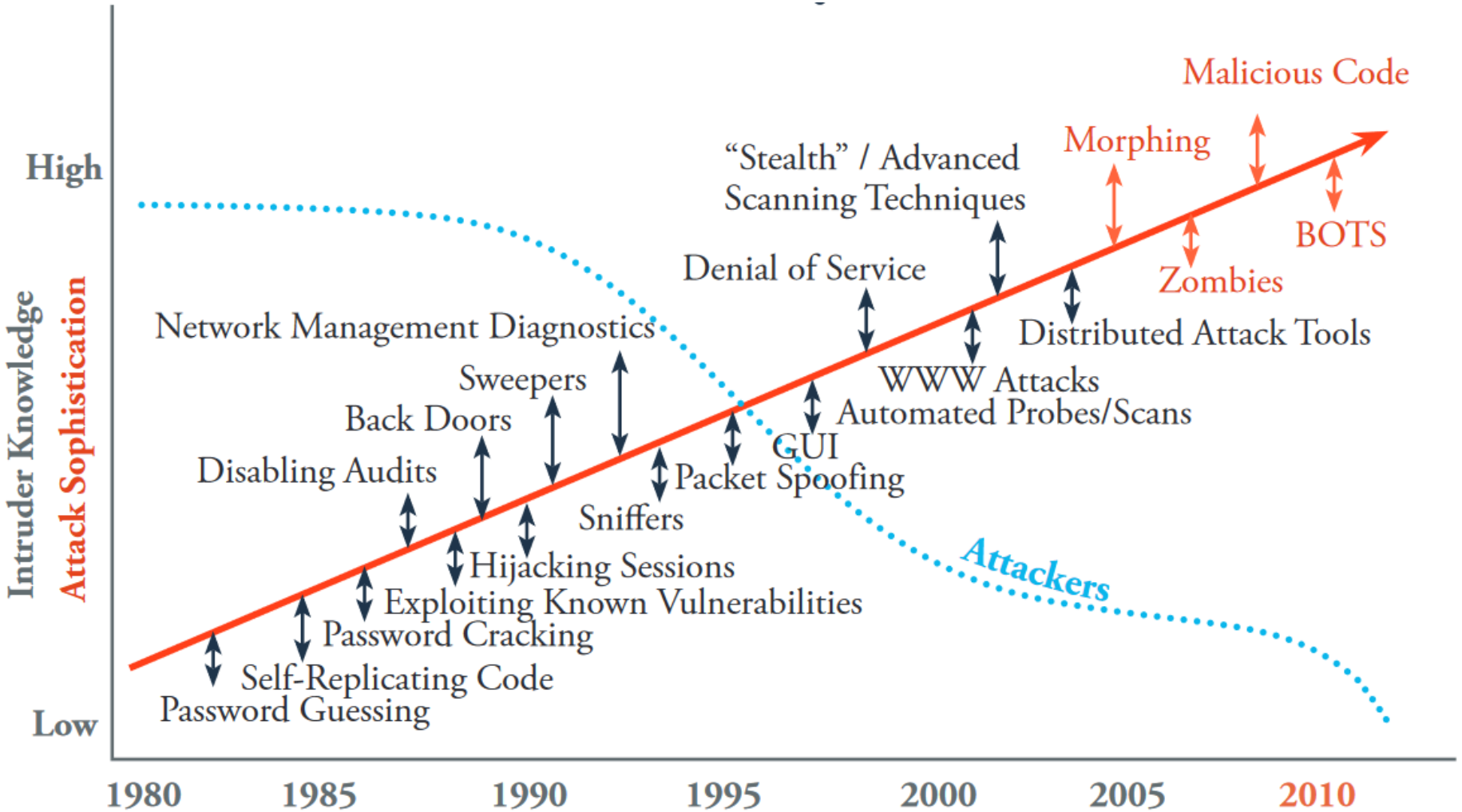
rnet users increasingly rely on encrypted tunnels to heir web browsing activities safe from eavesdrop- A typical scenario involves a user establishing an ted tunnel to a proxy that then relays all subsequent

manipulate whole streams of packets in order to precisely mimic the distribution of another website's packet lengths.

The seemingly widespread intuition behind these countermeasures is that they patch up the most dangerous side channel (packet lengths) and so provide good protection against TA attacks, including website identification. Existing literature might appear to support this intuition. For example, Liberatore and Levine [10] show that padding packets to the network MTU (e.g., 1500 bytes) reduces the accuracy of one of their attacks from 98% to 7%.

Our results strongly challenge this intuition. We perform the first comprehensive analysis of low-level countermeasures (e.g., per-packet padding) for the kind of website identification attacks considered by prior work (c.f., [8, 10, 14, 22]): a closed-world setting for privacy sets, in which the *a priori* set of possible websites a user might visit is known to the attacker, coupled with the ability for the attacker to train and test on traffic traces that are free of real-world artifacts (e.g., caching effects, interleaved flows, and user-specific content). We consider nine distinct countermeasures, apply them to two large, independent datasets of website downloads, and pit the resulting obfuscated traffic against a total of seven different attacks. The results are summarized in Figure 1. What we uncover is surprisingly bleak:

None of the countermeasures are effective. We show



Zdroj: 10.13140/RG.2.1.4774.9204

VPN

VPN

- důležitým identifikátorem je IP adresa
- *virtuální privátní síť* – k čemu to je?

- *jaké to má potíže?*
- zdarma = pomalé a *no*-no-log policy
- přenášení důvěry *(ISP -> VPN poskytovatel)*
- *cookies?* – není to buď/nebo…
- Netflix a *residential VPN*

transparency reports

[ExpressVPN]

[NordVPN]

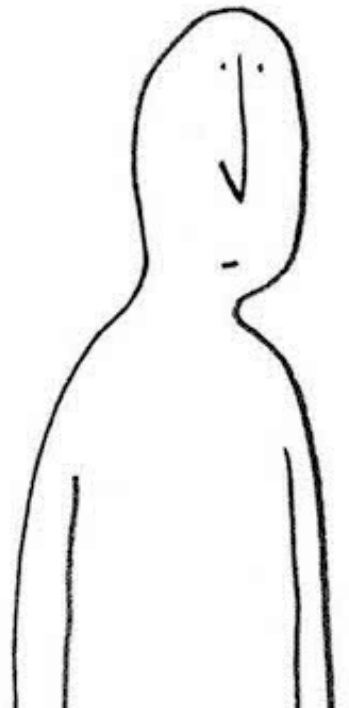
[CyberGhost]

[Proton VPN]

```
January 2019 – A data request from a foreign country was approved by the Swiss court system. However, as we do not have any customer IP information, we could not provide the requested information, and this was explained to the requesting party.
```

HLPčko...

- komerční VPN
- hostováno ve Švýcarsku
- transparentnost
- *dvousečná zbraň*

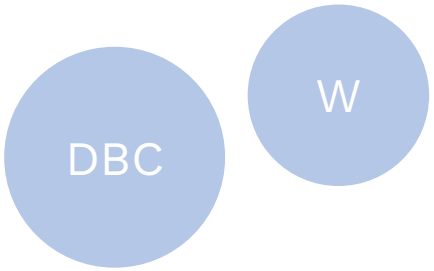


Onion routing a TOR

Platformy

Náš obsah leží jinde

- *Gmail, Facebook,...*
- přístup k vlastním datům?
- kontrola nad daty?
- nastavení soukromí?
- data leaks / breach
- have i been pwned?



Oh no — pwned!

Pwned in 30 data breaches and found 4 pastes (subscribe to search sensitive breaches)

Donate

Internet Archive: In September 2024, the digital library of internet sites Internet Archive suffered a data breach that exposed 31M records. The breach exposed user records including email addresses, screen names and bcrypt password hashes.

Compromised data: Email addresses, Passwords, Usernames

CNET YOUR GUIDE TO A BETTER FUTURE

Trending AI Tech Money Home Wellness Home Internet Deals

News > Privacy

Facebook Messenger bug revealed who you had conversations with

The browser flaw let potential attackers figure out whos
DMs you slid into.

Alfred Ng
March 7, 2019 4:07 p.m. PT

3 min re

naked security by SOPHOS

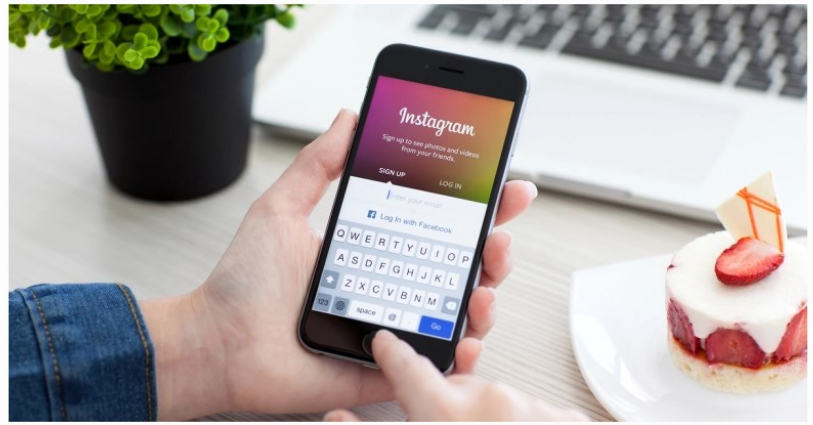
PRODUCTS › FREE TOOLS › FREE SOPHOS HOME ›

Have you listened to our podcast? Listen now

Instagram bug could have allowed others to read your direct messages

17 FEB 2016 3

Privacy, Social networks



Previous: "Locky" ransomware – what you need to know

Next: Apple says NO to iPhone backdoor in terror case

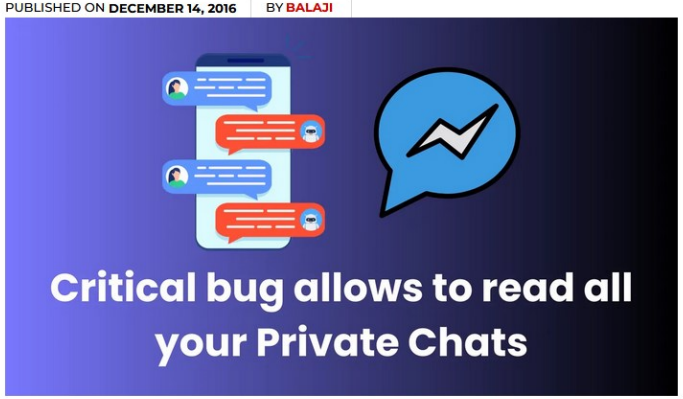
gbhackers.

Home › Data Breach ›

Critical bug allows to read all your Private Chats of Facebook Messenger by hackers

Data Breach Hacks Password Attacks

PUBLISHED ON DECEMBER 14, 2016 BY BALAJI



One of the network's most popular features, with 1-billion active monthly users. Unlike photo and status features designed specifically for sharing and publishing, the power of Messenger is in the ability to communicate privately.

security vulnerability found on Facebook, which also potentially affects millions of websites using origin null restriction checks, threatening user privacy and opening

FACEBOOK ENGINEERS: WE HAVE NO IDEA WHERE WE KEEP ALL YOUR PERSONAL DATA

In a discovery hearing, two veteran Facebook engineers told the court that the company doesn't keep track of all your personal data.

Sam Biddle

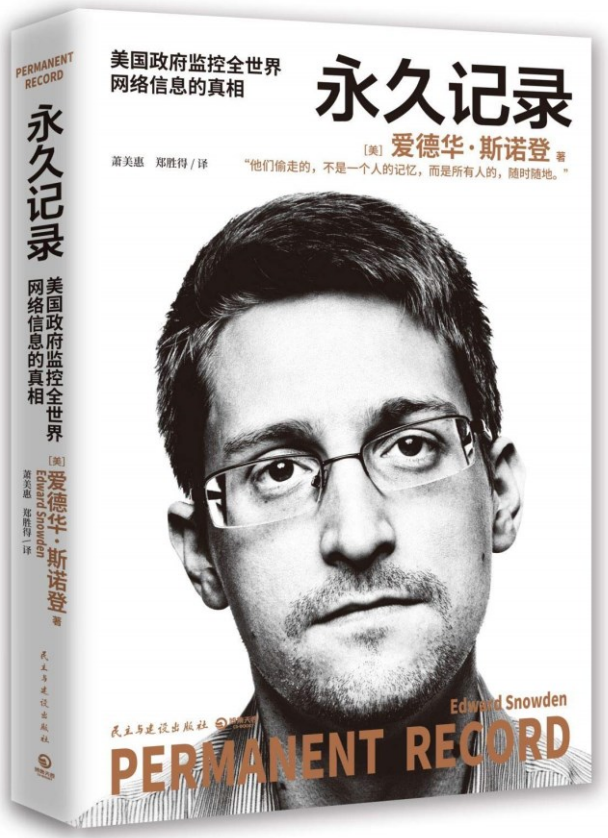
September 7 2022, 7:00 a.m.

Share

Co se stane po úniku dat?

- objeví se to venku
- často náhodně, často až po čase
- mnohdy k zakoupení
- začne se zkoušet, testovat, kombinovat
- ověřuje se pravdivost a aktuálnost
- *hledá se zdroj* – mnohdy kombinace
- reportuje se

backdoor


PERMANENT RECORD
永久记录
美国政府监控全世界网络信息的真相
[美]爱德华·斯诺登 著
萧美惠 郑胜得 译
永久记录
美国政府监控全世界网络信息的真相
[美]爱德华·斯诺登
Edward Snowden
著
萧美惠 郑胜得 译
民主与建设出版社
Edward Snowden
PERMANENT RECORD

TOP SECRET//SI//ORCON//NOFORN

PRISM/US-984XN Overview

OR

*The SIGAD Used **Most** in NSA Report*
Overview

[redacted]

April 2013

Derive

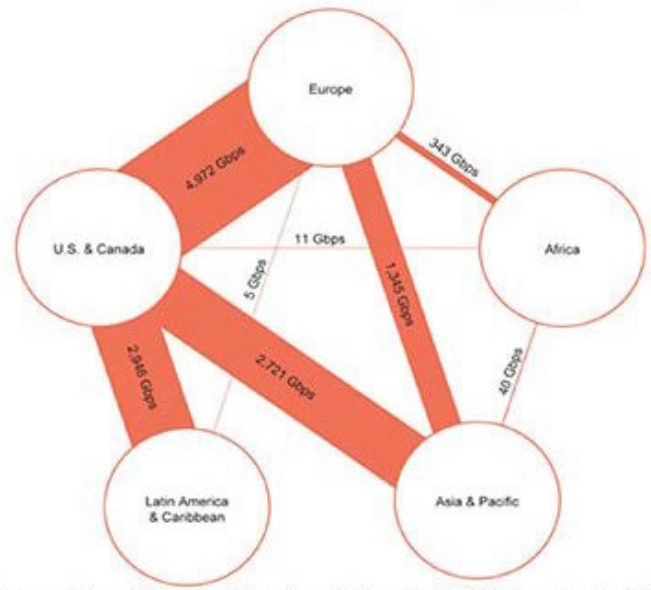
TOP SECRET//S

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



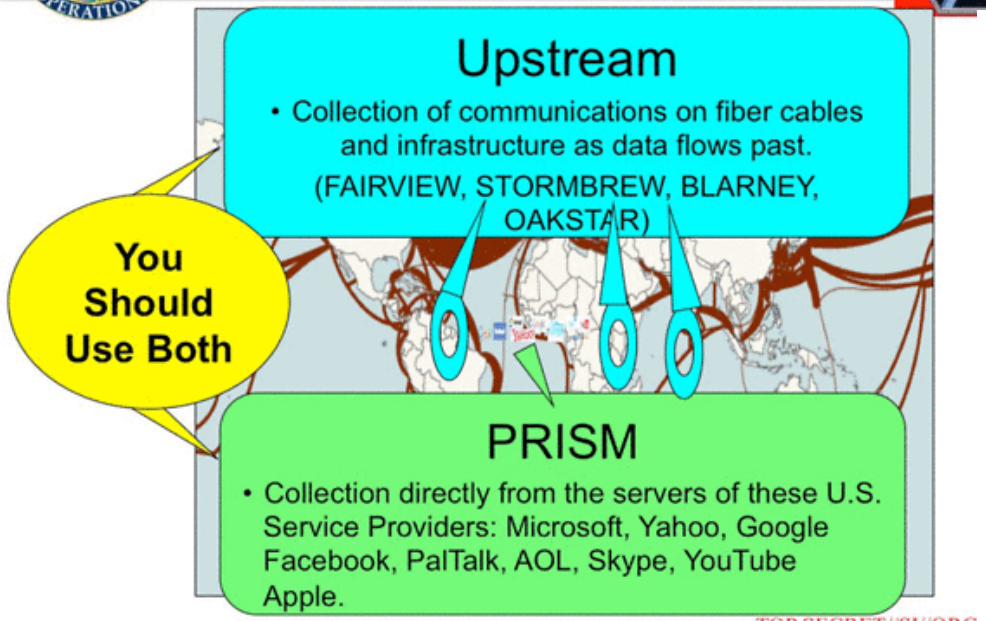
International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection



TOP SECRET//SI//ORC

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

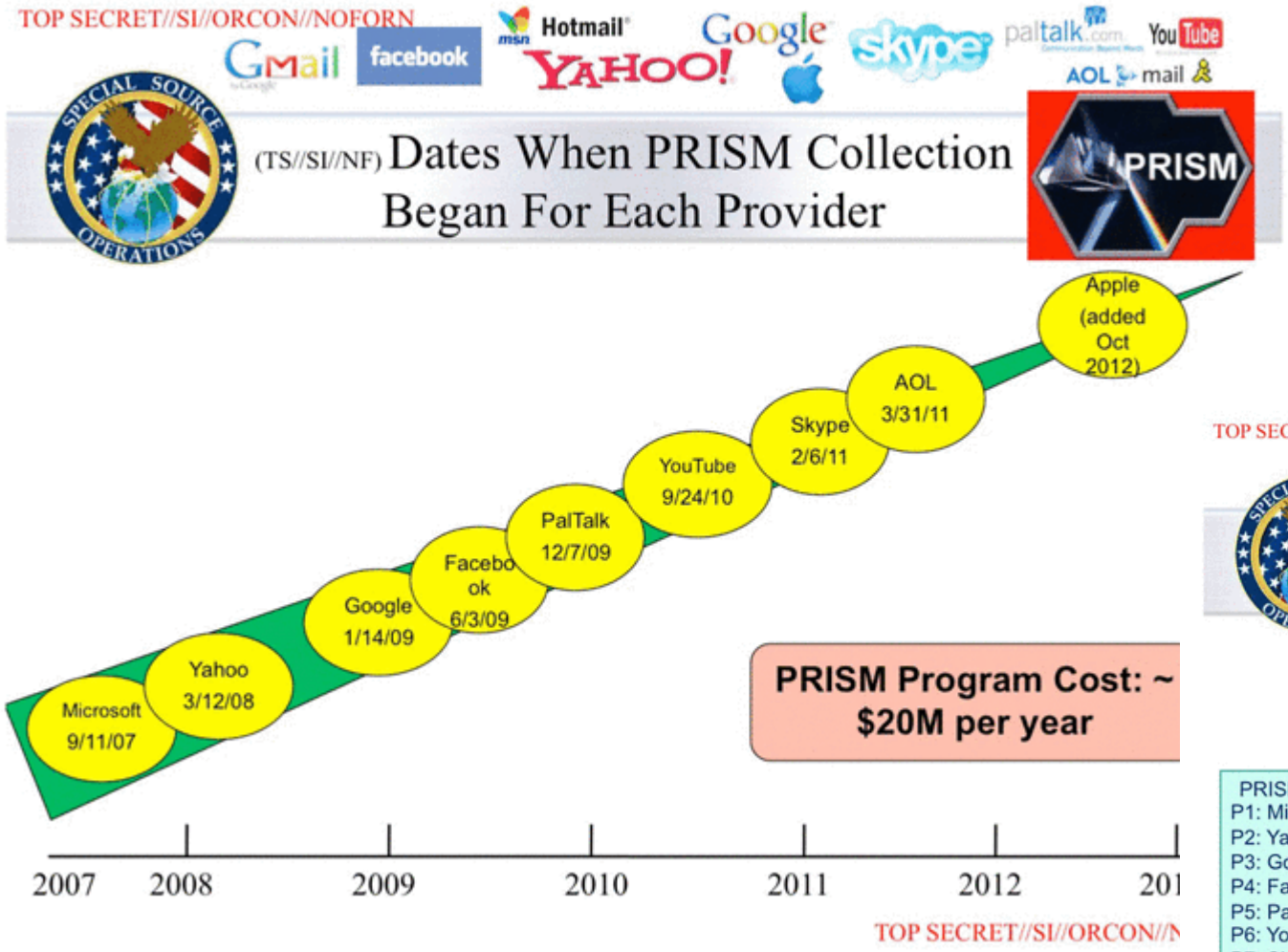
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

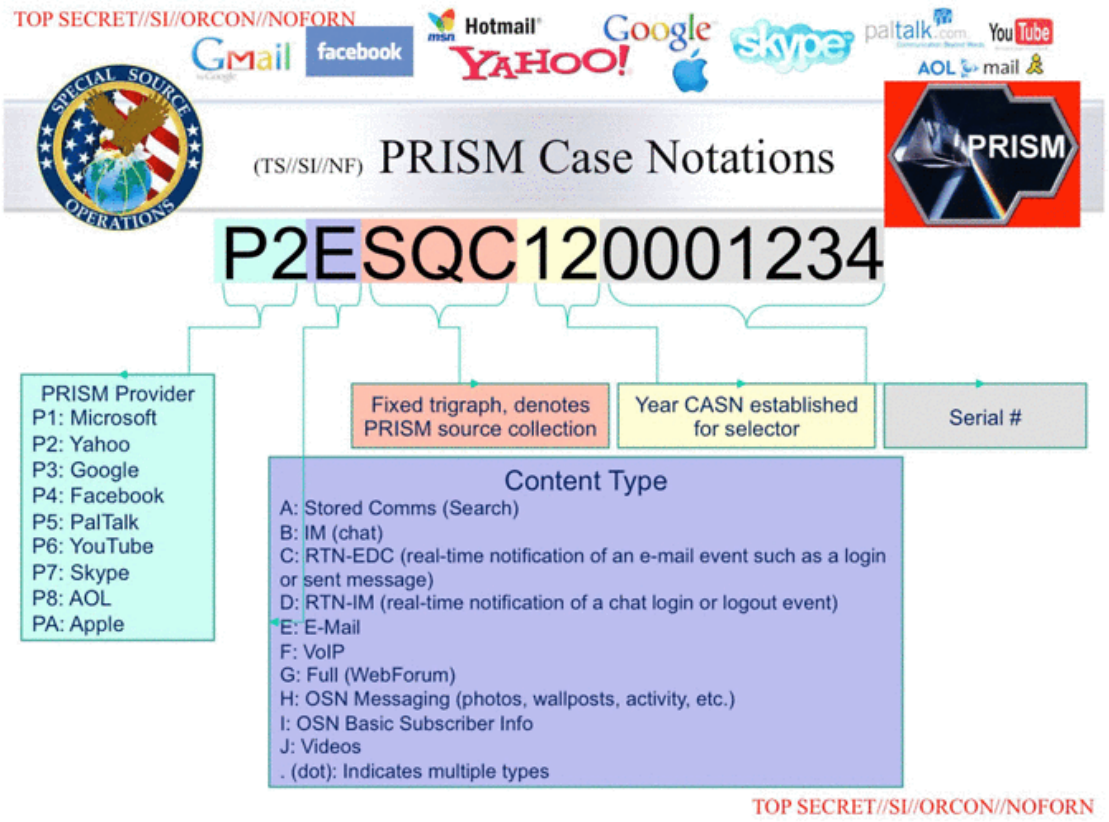
What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

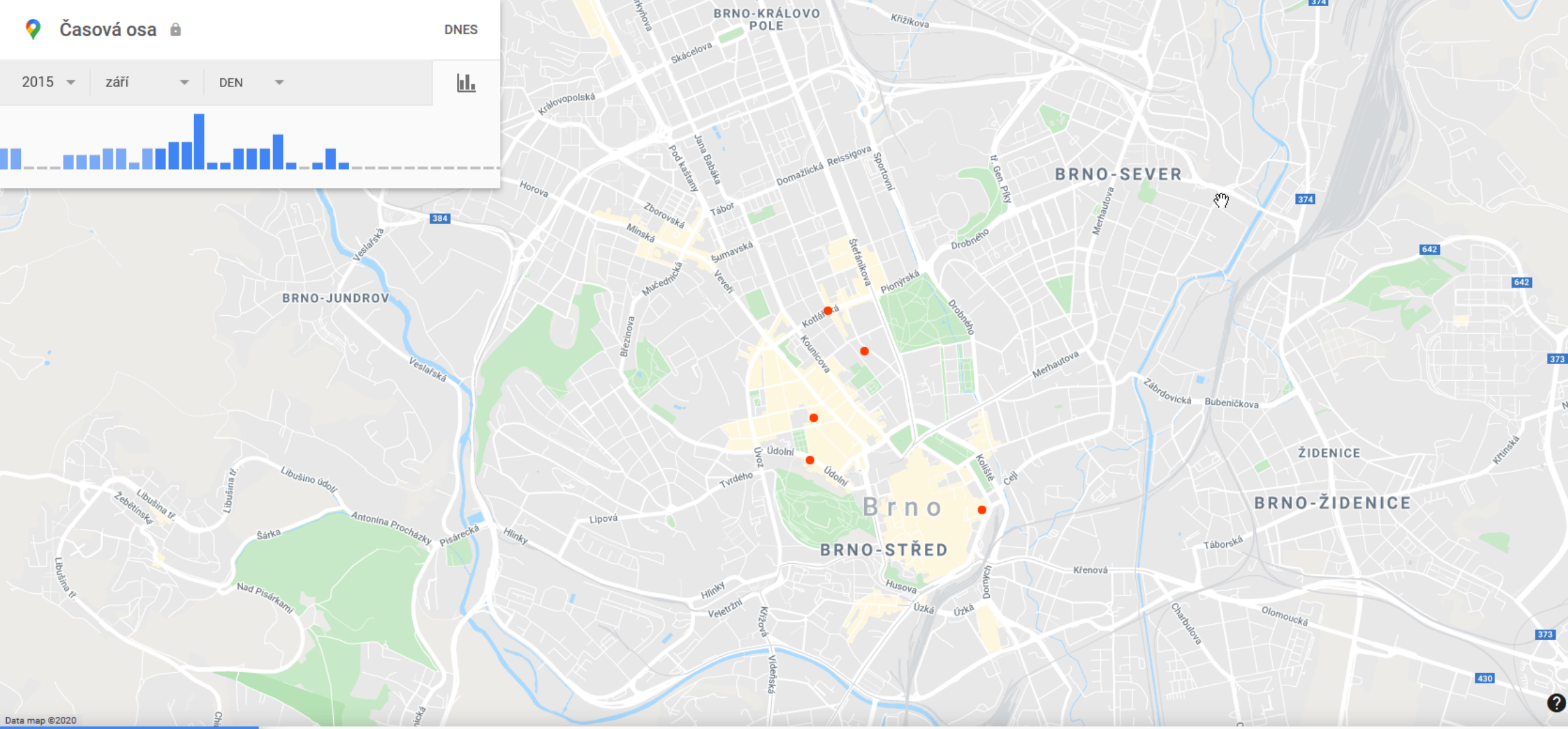

TOP SECRET//SI//ORCON//NOFORN
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
TOP SECRET//SI//ORCON//N


TOP SECRET//SI//ORCON//NOFORN
(TS//SI//NF) PRISM Case Notations
PRISM
P2ESQC120001234
PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple
Fixed trigraph, denotes PRISM source collection
Year CASN established for selector
Serial #
Content Type
A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types
TOP SECRET//SI//ORCON//NOFORN

XKeyscore

„You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information. ... You can tag individuals ... Let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a forum somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity.“

Zdroj: https://web.archive.org/web/20140128224439/http://www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html



září 2015

1 zajímavé místo

Odpoledne Taneční konzervatoř, Brno, Nejedlého 3

10. 9. 2015

Vyberte možnost automatického mazání pro Historii polohy

- (●) **Automaticky mazat aktivitu starší než 3 měsíce**
  a ručně lze smazat kdykoli
- ( ) **Automaticky mazat aktivitu starší než 18 měsíců**
  a ručně lze smazat kdykoli
- ( ) **Automaticky mazat aktivitu starší než 36 měsíců**
  a ručně lze smazat kdykoli
- ( ) **Nemazat automaticky**

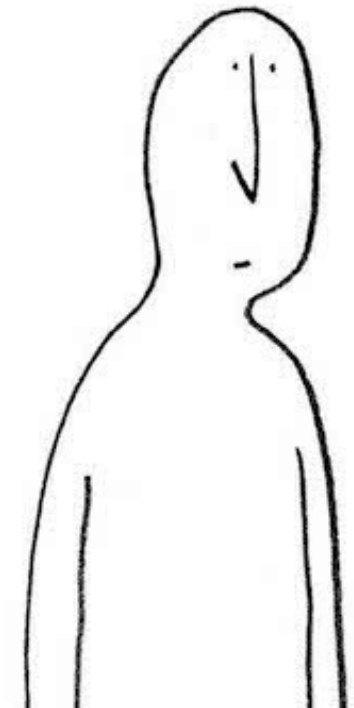
Jak dlouho?

Když uchováváte historii polohy, máte možnost zpětně dohledat navštívená místa i trasy, po kterých jste cestovali. Tato data můžete přestat ukládat pozastavením historie polohy.

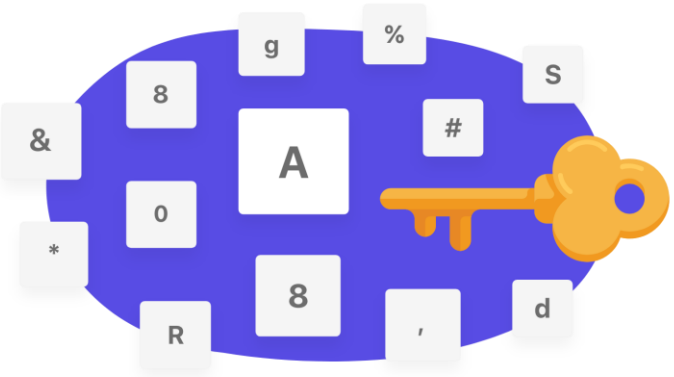
Další

HLPčko...

- proklikávám (pravidelně) nastavení soukromí
- snažím se dočíst, co které znamená
- nastaveny alerty na úniky dat
- po úniku kontroluji, co může být ohroženo



Odbočka: Hesla

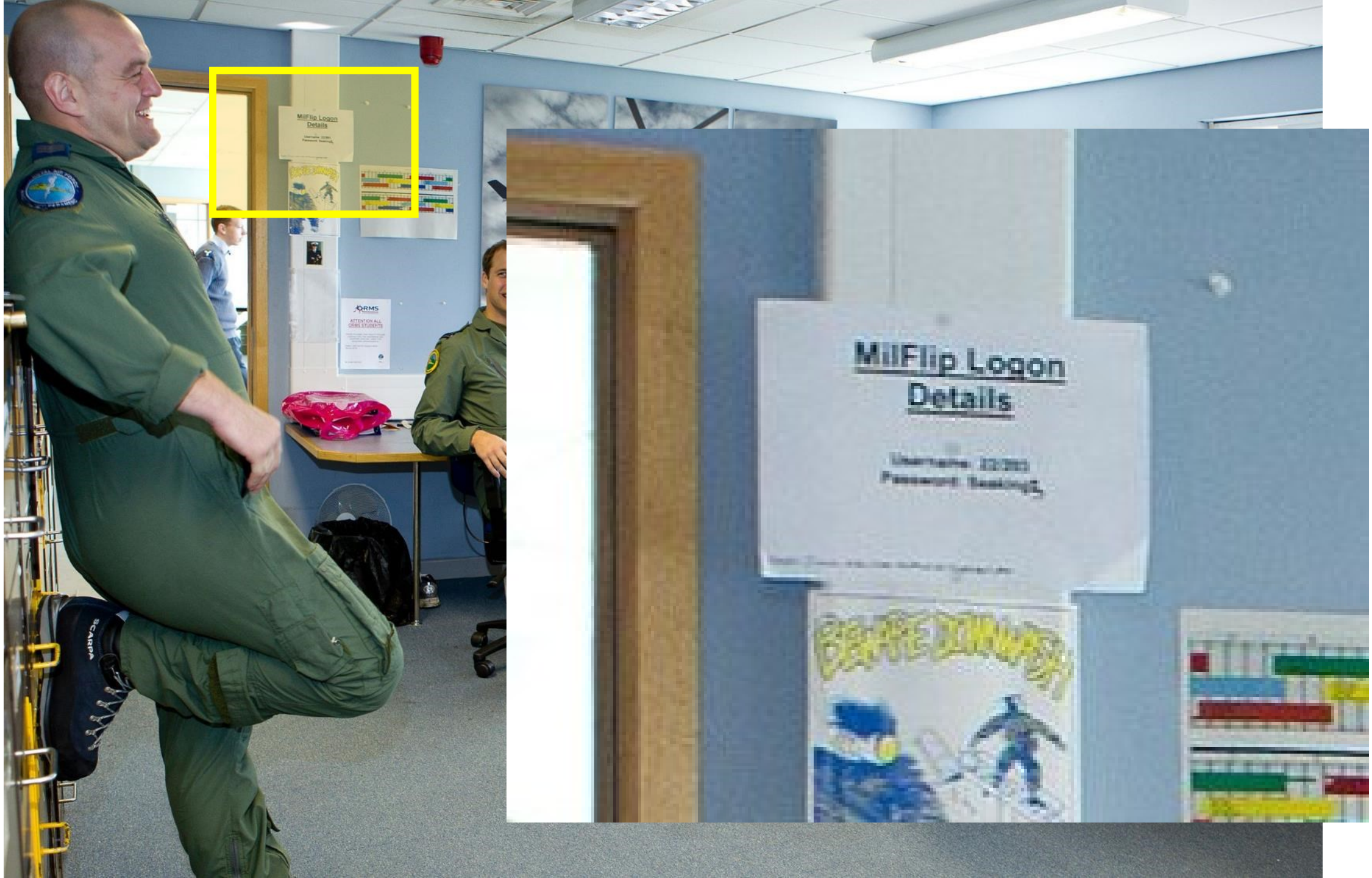


[passkeys](#)

paswordless

- pevná hesla?
- správci hesel – jaké to má potíže?
- 2FA *(knowledge, possession, inherent, location)*
- [Leaked Passwords](#)
- slovník / [brute force](#) / credential stuffing


MilFlip Logon Details
ATTENTION ALL ORMS STUDENTS
SCARPA


MilFlip Logon
Details

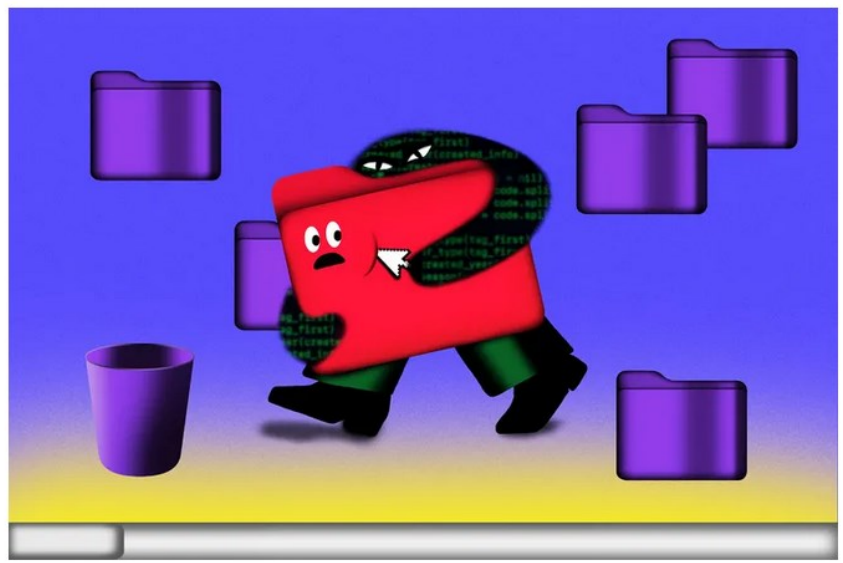
HLPčko...

- LastPass jako správce hesel
- silné unikátní heslo
- některá hesla jen v hlavě
- 2FA skrze HW klíč

- LastPass jako správce hesel

SECURITY / POLICY / TECH

Experts link LastPass security breach to a string of crypto heists



One researcher claims the number of victims who stored their crypto keys on LastPass was "simply too much to ignore." Illustration: Beatrice Sala

/ More than $35 million has been stolen from over 150 victims since December — 'nearly every victim' was a LastPass user.

By **Jess Weatherbed**, a news writer focused on creative industries, computing, and internet culture. Jess started her career at TechRadar, covering news and hardware reviews.

Sep 7, 2023, 12:45 PM GMT+2 | 16 Comments / 16 New

Šifrování

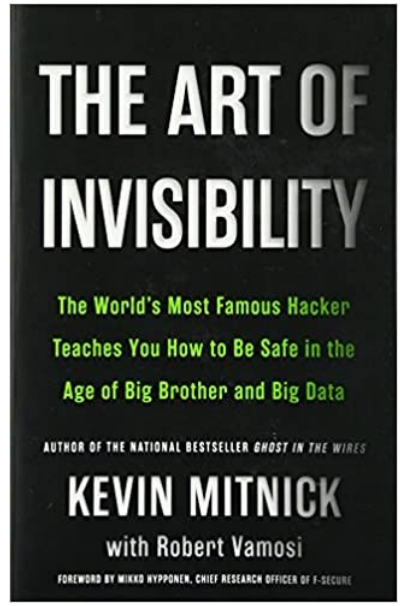
- *end-to-end šifrování*
- WhatsApp, Signal, Threema – *data v pohybu*
- *jaké to má potíže?*
- *kritický počet uživatelů*
- zadní vrátka
- má to jedno slabé místo…
- *šifrování dat na disku?* – USB paměť?

RM

EU

Ekosystém

Není to jen o PC



Každé nové zařízení zapadne do ekosystému.

- mobil jako vstupní brána do vašeho života
- mobil jako další zdroj dat – *všudypřítomný*
- geolokace

- anonymita? – *burner* – Kevin Mitnick
- IMSI CATCHER – Agáta

GSM

Není to jen o PC

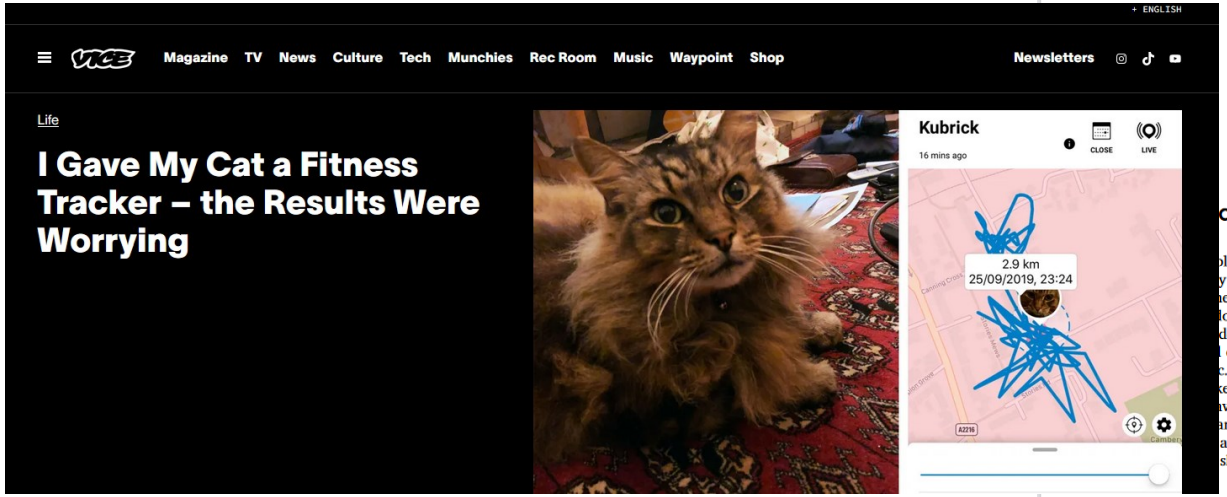
- IoT – internet věcí, chytrá zařízení
- IoT jako bezpečnostní problém
- IoT jako zdroj cenných dat - *Shodan*

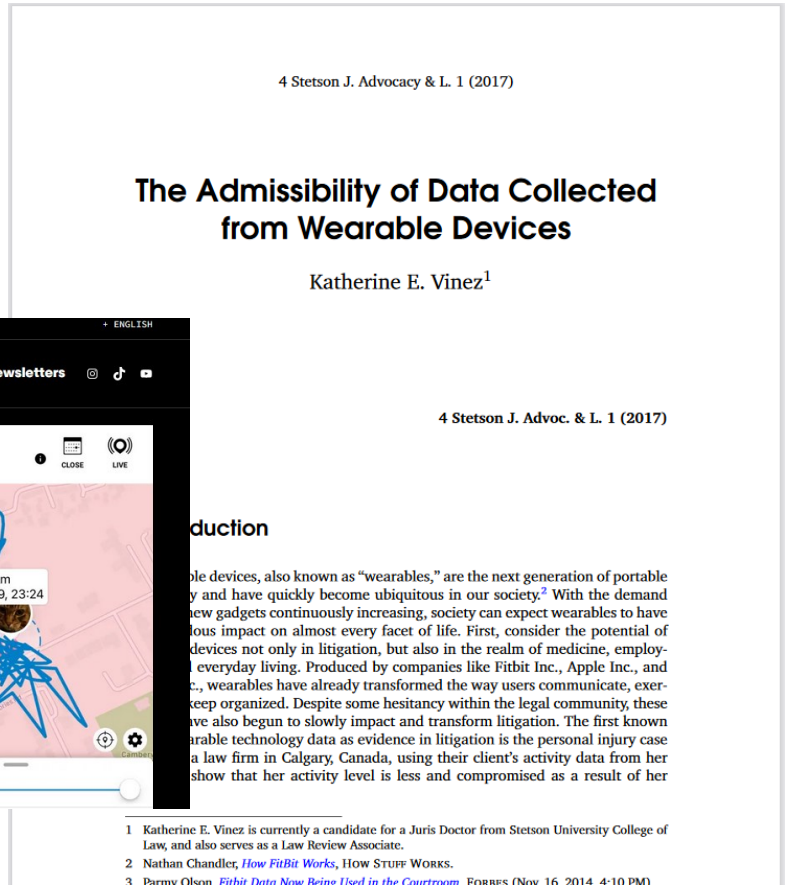
- chytrá žárovka

- chytrá města
- anonymizace a deanonymizace

Není to jen o PC

- wearables
- nositelné technologie
- *quantified self*





4 Stetson J. Advocacy & L. 1 (2017)

The Admissibility of Data Collected from Wearable Devices

Katherine E. Vinez[1]

4 Stetson J. Advoc. & L. 1 (2017)

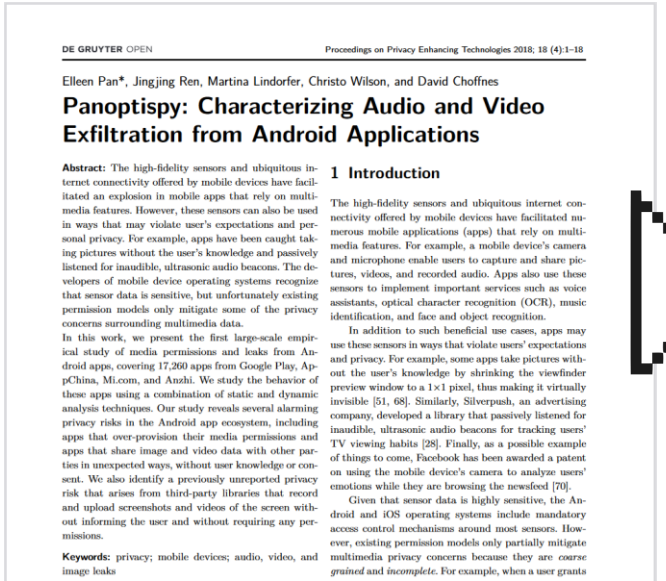
duction

ble devices, also known as "wearables," are the next generation of portable y and have quickly become ubiquitous in our society.[2] With the demand new gadgets continuously increasing, society can expect wearables to have dous impact on almost every facet of life. First, consider the potential of devices not only in litigation, but also in the realm of medicine, employ- everyday living. Produced by companies like Fitbit Inc., Apple Inc., and c., wearables have already transformed the way users communicate, exer- keep organized. Despite some hesitancy within the legal community, these ve also begun to slowly impact and transform litigation. The first known arable technology data as evidence in litigation is the personal injury case a law firm in Calgary, Canada, using their client's activity data from her show that her activity level is less and compromised as a result of her

1 Katherine E. Vinez is currently a candidate for a Juris Doctor from Stetson University College of Law, and also serves as a Law Review Associate.
2 Nathan Chandler, *How FitBit Works*, How Stuff Works.
3 Parmy Olson, *Fitbit Data Now Being Used in the Courtroom*, Forbes (Nov. 16, 2014, 4:10 PM)

Není to jen o PC

- IVA - Alexa, Cortana a podobné...
- bezpečnostní problémy



DE GRUYTER OPEN Proceedings on Privacy Enhancing Technologies 2018; 18 (4):1–18

Elleen Pan*, Jingjing Ren, Martina Lindorfer, Christo Wilson, and David Choffnes

Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications

Abstract: The high-fidelity sensors and ubiquitous internet connectivity offered by mobile devices have facilitated an explosion in mobile apps that rely on multimedia features. However, these sensors can also be used in ways that may violate user's expectations and personal privacy. For example, apps have been caught taking pictures without the user's knowledge and passively listened for inaudible, ultrasonic audio beacons. The developers of mobile device operating systems recognize that sensor data is sensitive, but unfortunately existing permission models only mitigate some of the privacy concerns surrounding multimedia data.

In this work, we present the first large-scale empirical study of media permissions and leaks from Android apps, covering 17,260 apps from Google Play, AppChina, Mi.com, and Anzhi. We study the behavior of these apps using a combination of static and dynamic analysis techniques. Our study reveals several alarming privacy risks in the Android app ecosystem, including apps that over-provision their media permissions and apps that share image and video data with other parties in unexpected ways, without user knowledge or consent. We also identify a previously unreported privacy risk that arises from third-party libraries that record and upload screenshots and videos of the screen without informing the user and without requiring any permissions.

Keywords: privacy; mobile devices; audio, video, and image leaks

1 Introduction

The high-fidelity sensors and ubiquitous internet connectivity offered by mobile devices have facilitated numerous mobile applications (apps) that rely on multimedia features. For example, a mobile device's camera and microphone enable users to capture and share pictures, videos, and recorded audio. Apps also use these sensors to implement important services such as voice assistants, optical character recognition (OCR), music identification, and face and object recognition.

In addition to such beneficial use cases, apps may use these sensors in ways that violate users' expectations and privacy. For example, some apps take pictures without the user's knowledge by shrinking the viewfinder preview window to a 1×1 pixel, thus making it virtually invisible [51, 68]. Similarly, Silverpush, an advertising company, developed a library that passively listened for inaudible, ultrasonic audio beacons for tracking users' TV viewing habits [28]. Finally, as a possible example of things to come, Facebook has been awarded a patent on using the mobile device's camera to analyze users' emotions while they are browsing the newsfeed [70].

Given that sensor data is highly sensitive, the Android and iOS operating systems include mandatory access control mechanisms around most sensors. However, existing permission models only partially mitigate multimedia privacy concerns because they are *coarse grained* and *incomplete*. For example, when a user grants

Není to jen o PC

- síťový HW
- https://upc.michalspacek.cz/

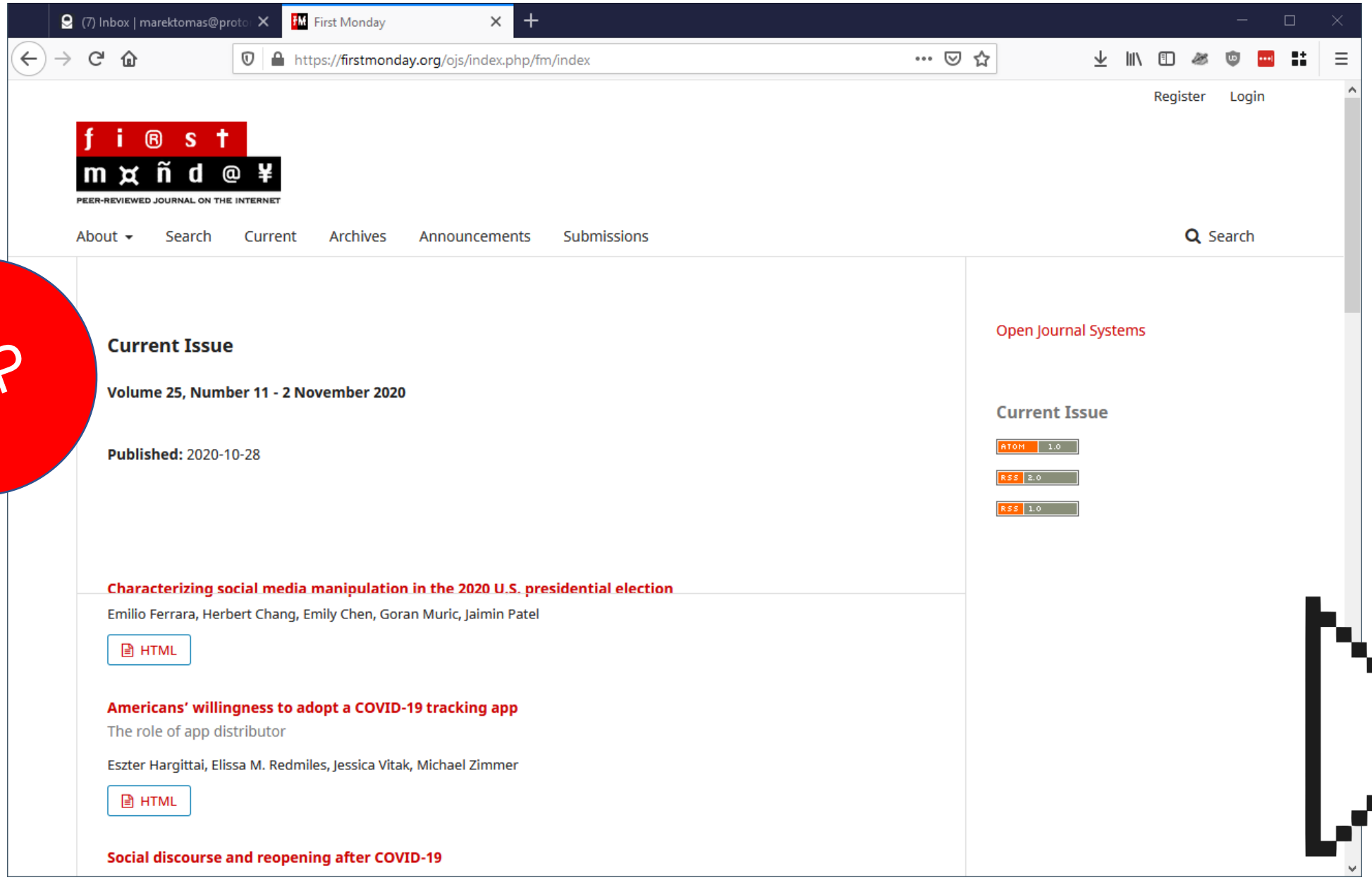
- fotoaparáty - EXIF informace
- geolokace
- webkamera

čím více bezpečí a anonymity,
tím více nepohodlí

Co teď s tím vším?


#FALLONTONIGHT

TIP


(7) Inbox | marektomas@proto
First Monday
https://firstmonday.org/ojs/index.php/fm/index
Register
Login
first monday
PEER-REVIEWED JOURNAL ON THE INTERNET
About
Search
Current
Archives
Announcements
Submissions
Search
Current Issue
Volume 25, Number 11 - 2 November 2020
Published: 2020-10-28
Characterizing social media manipulation in the 2020 U.S. presidential election
Emilio Ferrara, Herbert Chang, Emily Chen, Goran Muric, Jaimin Patel
HTML
Americans' willingness to adopt a COVID-19 tracking app
The role of app distributor
Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, Michael Zimmer
HTML
Social discourse and reopening after COVID-19
Open Journal Systems
Current Issue
ATOM 1.0
RSS 2.0
RSS 1.0